Universidad Carlos III de Madrid

Departamento de Ingeniería Telemática

Redes de Ordenadores

Prácticas de captura de tráfico

Grado en Ingeniería Informática

1. Objetivo

El objetivo de esta práctica es profundizar en el conocimiento de los protocolos más importantes del modelo TCP/IP vistos en la asignatura, empleando diversas aplicaciones del sistema operativo que las implementan, así como el capturador de tráfico / analizador de paquetes (*Wireshark* - *http://www.wireshark.org/*) utilizado en la práctica de concepto 1 (DNS).

2. Descripción

A lo largo de la práctica se va a profundizar en conceptos fundamentales de protocolos correspondientes a distintos niveles del modelo TCP / IP. Concretamente, se estudiarán protocolos del nivel de enlace, del nivel de red y del nivel de transporte. En el nivel de enlace nos centraremos en Ethernet y ARP. Para el nivel de red, el análisis se realizará sobre IPv4. Finalmente para el nivel de transporte se estudiarán características del protocolo TCP.

Con el objetivo de hacer esta práctica fácil de realizar se han elegido una serie de aplicaciones existentes en los sistemas operativos *GNU Linux* y *Microsoft Windows* (la práctica puede hacerse en ambos sistemas operativos). Cabe destacar que el uso de algunos de los comandos es diferente en base al sistema operativo empleado.

La práctica ha sido dividida en varias dos partes independientes, entre las que se reparten una serie de pruebas, correspondientes a cada uno de los niveles expuestos anteriormente.

2.1. Parte I [Niveles de transporte y red]

IMPORTANTE: La memoria en la que se respondan las preguntas deberá ser entregada **como máximo 10 minutos después** de finalizada la **primera** sesión de captura a través del entregador habilitado a tal efecto en Aula Global 2.

2.1.1. – Nivel de transporte

En este apartado se va a analizar uno de los principales protocolos del nivel de transporte empleado en Internet, el *Transmission Control Protocol* (TCP). Siga los siguientes pasos:

1.- Abra Wireshark y póngalo a capturar en la interfaz correspondiente.

2.- Acceda **a una** de las siguientes direcciones: http://goo.gl/wFwVD o http://goo.gl/grDQf

3.- Ponga a reproducir el vídeo.

4.- Al cabo de unos cuantos segundos (**menos de un minuto**) detenga la captura.

Responda las siguientes preguntas:

P1) Identifique los mensajes correspondientes al proceso de "three-way-handshake" de establecimiento de conexión con la web. ¿Qué información se intercambia en cada uno de ellos? ¿Cuáles son los números de secuencia y de ACK en cada mensaje? Adjunte una captura de pantalla.

P2) Identifica el primer mensaje enviado una vez realizado el "three-way-handshake". ¿Cuáles son la IP y puerto de origen del mensaje? ¿Y la IP y puerto de destino? ¿Qué número de secuencia tiene el mensaje? ¿Cuál será el número de ACK esperado en la respuesta a este mensaje?

P3) ¿El vídeo se transmite a través del protocolo de transporte TCP o UDP? ¿Por qué cree que esto es así?

P4) Identifique el primer mensaje enviado en la descarga del flujo de vídeo. ¿Cuál es la IP del servidor remoto que transmite el vídeo? ¿Cuál es el puerto de destino de la conexión? ¿Y el puerto origen? Adjunte una captura de pantalla.

P5) Seleccione un paquete correspondiente a los datos de vídeo y a continuación genere una gráfica del "Throughput" para el flujo de información en el que viajaba dicho paquete (Statistics → TCP Stream Graph → …). Adjúntela como captura de pantalla e indique por qué cree que la gráfica tiene ese aspecto.

Sobre la gráfica obtenida en la P5:

P6) ¿Cuánto tiempo aproximado se ha estado recibiendo vídeo?

P7) ¿Cuál ha sido la velocidad media de descarga de vídeo? ¿Ha sido dicha velocidad más o menos constante a lo largo del tiempo o ha sido irregular? ¿Por qué cree que ha sido así? Justifique todas las respuestas.

2.1.2. – Nivel de red

En este apartado se va a analizar uno de los principales protocolos del nivel de red, el *Internet Protocol* (IP). Más concretamente IPv4. Los pasos a seguir para poder contestar a las preguntas correspondientes son los siguientes:

1.- Abrir Wireshark y a continuación una consola de comandos.

2.- Escribir en la consola el comando necesario para realizar un ping a la puerta de enlace predeterminada del equipo (IP del router que brinda al equipo acceso a la red)**. ¡No ejecutar todavía!**

3.- Poner a capturar Wireshark en la interfaz correspondiente.

4.- Ejecutar el comando que estaba escrito en la consola de comandos.

5.- Tras capturar unos cuantos mensajes de ping, detener la captura.

P1) ¿Cuál es el tamaño total del mensaje ICMP? ¿Cuántos datos se envían dentro del mensaje ICMP? Describa cuánto ocupa cada parte del mensaje.

P2) ¿Cuál es el puerto origen y destino del mensaje ICMP? ¿Por qué cree que es así? Justifique las respuestas.

Repita los pasos anteriores, pero esta vez envíe **60000 bytes** en cada mensaje. Conteste las siguientes preguntas:

P3) Explique detalladamente cómo ha cambiado la situación ahora con respecto a la prueba anterior.

P4) Localice el fragmento en el que está la cabecera del mensaje ICMP (adjunte captura de pantalla significativa).

P5) ¿Por qué no se recibe ninguna respuesta hasta que el destino no ha recibido todos los fragmentos en lugar de contestar uno a uno?

P6) ¿Cuál es el contenido del campo de datos? Indique el sistema operativo sobre el que ha realizado la prueba.

2.2. Parte II [Nivel de enlace]

IMPORTANTE: La memoria en la que se respondan las preguntas deberá ser entregada **como máximo 10 minutos después** de finalizada la **segunda** sesión de captura a través del entregador habilitado a tal efecto en Aula Global 2.

2.2.1. Ethernet

Para poder contestar las preguntas lleve a cabo los siguientes pasos:

1.- Abrir Wireshark y a continuación una consola de comandos.

2.- Escribir en la consola el comando necesario para realizar un ping a la puerta de enlace predeterminada del equipo (IP del router que brinda al equipo acceso a la red)**. ¡No ejecutar todavía!**

3.- Poner a capturar Wireshark en la interfaz correspondiente.

4.- Ejecutar el comando que estaba escrito en la consola de comandos.

5.- Tras capturar unos cuantos mensajes de ping, detener la captura de paquetes en Wireshark.

Conteste las siguientes preguntas:

P1) ¿Cuál es la dirección MAC de origen y de destino en el mensaje ICMP?

P2) ¿Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.

P3) ¿Qué significan los flags del mensaje ICMP en la capa Ethernet?

Vuelva a repetir los pasos del 1 al 5, pero esta vez, realice el ping a www.google.com. Conteste las siguientes preguntas:

P4) ¿Cuál es la dirección MAC de origen y de destino en el mensaje ICMP?

P5) ¿Puede ver en el mensaje la dirección IP de Google? ¿Y su MAC? Justifique todas las respuestas.

2.2.2. ARP

*P6) Haciendo uso del comando **arp**, obtenga la tabla ARP de la máquina. Describa los distintos campos y adjunta una captura de pantalla.*

Siga los siguientes pasos:

1.- Abrir la aplicación Wireshark y poner a capturar en la interfaz correspondiente.

2.- Ejecute un ping a www.google.com.

3.- Tras capturar unos cuantos mensajes de ping, detener la captura.

P7) Localice todos los mensajes que han permitido obtener la IP de Google (tanto DNS como ARP), y justifique cómo se ha podido llevar a cabo, paso a paso, la identificación del mismo.

Ahora siga los siguientes pasos:

1.- Abrir la aplicación Wireshark y poner a capturar en la interfaz correspondiente.

2.- Ejecutar en una consola de comandos lo siguiente:

En Windows:

```
netsh interface ip delete arpcache
ipconfig /flushdns
```

En Linux:

```
sudo ip neigh flush dev eth0
sudo /etc/init.d/nscd restart
```

3.- Ejecutar un ping a www.google.com

4.- Tras unos cuantos mensajes de ping, detener la captura.

P8) Explique para qué sirven los comandos del paso 2.

P9) Localice todos los mensajes que han permitido obtener la IP de Google (tanto DNS como ARP). ¿Ha cambiado algo respecto al caso analizado en la P7? Justifique la respuesta.

2.2.3. Envenenamiento ARP

Abra un terminal e introduzca, mediante los comandos apropiados, una entrada en la tabla ARP de forma que a la hora de hacer ping desde el host 'A' a otro host del aula 'B', en vez de llegar el mensaje a 'B' (como sería lógico) llegue a 'A'. Capture esto con Wireshark.

P10) Adjunte capturas de pantalla significativas en las que se muestre la nueva tabla ARP y los mensajes capturados por Wireshark. Describa el procedimiento empleado para conseguir el desvío de tráfico propuesto, indicando los comandos utilizados y justificando su uso.

3. Consejos y buenas prácticas

- A la hora de hacer las capturas, intentar tener el mínimo número de aplicaciones corriendo que hagan uso de la red. Es inevitable que existan servicios corriendo en segundo plano, como el que se ocupa de mantener el sistema de fichero en red bajo las cuentas de Linux, pero siempre se pueden cerrar otras aplicaciones innecesarias que lo único que van a hacer es meter "ruido" en la captura y hacer más complejo el proceso de análisis.

- Utilizar la herramienta de filtros incorporada en Wireshark. Se pueden consultar cómo construir filtros tanto en el manual de usuario de la aplicación como en la ayuda on-line. El uso de esta herramienta os va a ahorrar muchos problemas y tiempo.

- Revisar bien los comandos que necesitáis (así como sus opciones) y aseguraros de tener un plan de acción antes de empezar con la práctica "a lo loco". Pensad qué datos necesitáis para hacer según qué cosas, qué comandos pueden resultar más útiles y llevaros menos tiempo y finalmente probarlo.

4. Requisitos

Para aprobar la práctica es necesario cumplir los siguientes requisitos:

- Se deberán contestar cuestiones de todas las partes de la práctica.
- Las respuestas a las cuestiones se entregarán en un documento **.pdf** a través de la actividad habilitada al efecto en Aula Global 2. El nombre de dicho fichero debe seguir el siguiente formato:

  RO-PCdPW-*[parte]*-*[id. de grupo]*.pdf

  Donde *"parte"* es un número entero correspondiente a la parte realizada (1 ó 2), y el *"identificador de grupo de alumnos"* estará compuesto de la siguiente forma:

  XY-Z

  Tal que:

  - **X** letra '**L**' o '**C**' correspondiente al campus (*Leganés* o *Colmenarejo*).
  - **Y** grupo (**80, 81, 82, 83, 84, 85, 89**).
  - **Z** número identificador de pareja de alumnos.

  Así pues, un ejemplo válido sería: **RO-PCdPW-1-L81-5.pdf**

- Se admiten también entregas en las que la memoria vaya comprimida en alguno de los formatos más comunes (zip, rar, tar.gz, 7z...). Siempre y cuando se respete el criterio de nombrado.

5. Normas

Para esta práctica se han establecido las siguientes normas:

- El documento entregado debe presentar una **portada** en la que figuren **el identificador de la pareja de alumnos** y sus **nombres**. Cada cuestión contestada debe ir precedida de su enunciado.
- Las prácticas que no tengan al menos la mitad de las cuestiones correctamente contestadas estarán suspensas, y su calificación dependerá del número de respuestas acertadas.
- Las prácticas entregadas fuera de plazo tendrán una calificación de 0 puntos.
- Las prácticas entregadas con un criterio de nombres distinto al establecido verán su nota reducida entre 0.5 y 2.5 puntos.